UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,147	08/27/2004	Lynn Henry Wheeler	10399-40263	5146

24728 7590 02/05/2008

MORRIS MANNING MARTIN LLP
3343 PEACHTREE ROAD, NE
1600 ATLANTA FINANCIAL CENTER
ATLANTA, GA 30326

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
02/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/711,147	WHEELER ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-37 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for a priority based on a U.S. application No. 09/189,159 filed on November 9, 1998.

Claim Objections

3. Claim 32 is objected to because of the following informalities: "record" should read "records". Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-37 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-37 of copending Application No. 10/711,149. Although the conflicting claims are not identical, they are not patentably distinct from each other claims of application 10/711,147 anticipate and/or are an obvious variation of claims of the application 10/711,149. For example see claims 1 and 3:

Application 10/711,147		**Application 10/711,149**
[Claim 1] In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of: (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information, and wherein the public key is associated with the account in a computer database; and thereafter (b) receiving the electronic communication from the sender, (i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a), (ii) wherein the electronic communication comprises, (A) the sender identity information, and (B) a digital signature derived from an electronic message using the private key of the pair, and (iii) wherein the electronic communication is		[Claim 1] In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of: (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information, and wherein the public key is associated with the account in a computer database; and thereafter (b) receiving the electronic communication from the sender, (i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a), (ii) wherein the electronic communication comprises, (A) the sender identity information, and (B) a digital signature derived from an electronic message using the private key of the pair from **and electronic message possessed first by the sender before the receiver, the sender identity information**

communicated electronically from the sender; and (c) validating the identity of the sender for the electronic communication by only performing the steps of, (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and (ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender		**being different from the electronic message**, and (iii) wherein the electronic communication is communicated electronically from the sender; and (c) validating the identity of the sender for the electronic communication by only performing the steps of, (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and (ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender.
[Claim 3] In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of: (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information and the sender identity information comprises other than an account number, and wherein the public key is associated with the account in a computer database; and thereafter (b) receiving the electronic communication from the sender, (i) wherein the electronic communication was		[Claim 3] In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of: (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information and the sender identity information comprises other than an account number, and wherein the public key is associated with the account in a computer database; and thereafter (b) receiving the electronic communication from the sender, (i) wherein the electronic communication was

created after the association of the sender identity information and the public key with the account in step (a), (ii) wherein the electronic communication comprises, (A) the sender identity information, and (B) a digital signature derived from an electronic message using the private key of the pair, and (iii) wherein the electronic communication is communicated electronically from the sender; and (c) validating the identity of the sender for the electronic communication by, (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and (ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender.		created after the association of the sender identity information and the public key with the account in step (a), (ii) wherein the electronic communication comprises, (A) the sender identity information, and (B) a digital signature derived from an electronic message using the private key of the pair **from and electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message**, and (iii) wherein the electronic communication is communicated electronically from the sender; and (c) validating the identity of the sender for the electronic communication by (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and (ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender.	

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

5. Claims 1-37 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-37 of U.S. Patent No. 6820202 and U.S. Patent No. 6820199 as well as claims 1-38 of U.S. Patent No. 7032112 and U.S. Patent No. 7089421 and claims 1-44 of U.S. Patent No. 7257228. Although the

conflicting claims are not identical, they are not patentably distinct from each other. For example the limitation: calculating hash value of the electronic message" recited in the independent claims of the patent 6820202 would have been at least implicit. A digital signature is created by first generating a hash of a message then encrypting with a private key. A corresponding public key is used to validating the private key/identity of the sender.

To give an additional comparison of claim language, see the claim language of the current application and patent 7,257,228, for example:

Application 10/711,147		**Patent 7,257,228**
[Claim 1] In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of: (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, **wherein the account comprises entity information**, and wherein the public key is associated with the account in a computer database; and thereafter (b) receiving the electronic communication from the sender, (i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a), (ii) wherein the electronic communication comprises, (A) the sender identity information, and		[Claim 1] In a system for performing an action, n response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of: (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, and wherein the public key is associated with the account in a computer database; and thereafter (b) receiving the electronic communication from the sender, (i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a), (ii) wherein the electronic communication comprises, (A) the sender identity information, and

(B) a digital signature derived from an electronic message using the private key of the pair, and (iii) wherein the electronic communication is communicated electronically from the sender; and (c) validating the identity of the sender for the electronic communication by only performing the steps of, (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and (ii) comparing a function of the public key and **the digital signature** with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting **the digital signature** using the public key, whereby a comparison resulting in a match validates the identity of the sender.		(B) predetermined encoded information obtained by using the private key of the pair, and (iii) wherein the electronic communication is communicated electronically from the sender; and (c) validating the identity of the sender for the electronic communication by only performing the steps of, (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and (ii) comparing a function of the public key and **the predetermined encoded information** with a function of the electronic message, wherein the function comprises decrypting the **predetermined encoded information** using the public key, whereby a comparison resulting in a match validates the identity of the sender.

A full detail comparison would be provided upon finality of double patenting rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Wheeler (UPSN 6820202),

Menezes et al. (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237), pg. 28-30.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/31/08

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER